I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIN IN AN ENVELOPE ADDRESSED TO: COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450, ON THE DATE INDICATED BELOW.

By: Lynn Lyons Date: March 9, 2006

MAIL STOP AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Application of: Lauri Paatero			
Conf. No.:	7915	Group Art Unit:	2137
Appln. No.:	10/047,193	Examiner:	Paul E. Callahan
Filing Date:	January 15, 2002	Attorney Docket No.:	9943-3 (2990568US/HM)

Title: METHOD OF PRODUCING A RESPONSE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Applicant requests review of the final rejection mailed September 9, 2005 in the above-identified application. No amendments are being filed with this request. This request is being filed with a Notice of Appeal. The review is requested for the reasons stated on the attached sheets.

Respectfully submitted,

LAURI PAATERO

March 9, 2006 By: _____
(Date)

LOUIS SICKLES II
Registration No. 45,803
AKIN GUMP STRAUSS HAUER & FELD LLP
One Commerce Square
2005 Market Street, Suite 2200
Philadelphia, PA 19103-7013
Telephone: 215-965-1200
Direct Dial: 215-965-1294
Facsimile: 215-965-1210
E-Mail: lsickles@akingump.com

LS
Enclosures

REMARKS IN SUPPORT OF PRE-APPEAL BRIEF REQUEST FOR REVIEW

Claims 9-16, as amended, are pending in this application. Claims 1-8 have been canceled. Claims 9, 10, 12, and 14-16 stand rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 4,471,216 (Herve) and U.S. Patent No. 5,604,810 (Dolan et al.). Claims 11 and 13 stand rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 4,471,216 (Herve) and U.S. Patent No. 5,604,810 (Dolan et al.) and further in view of WO 99/35782 (Kocher).

Rejection of claims 9, 10, 12, and 14-16 over U.S. Patent No. 4,471,216 (Herve) and U.S. Patent No. 5,604,810 (Dolan et al.).

In respect to claims 9, 10, 12 and 14-16, the Examiner expressly admits that Herve does not teach "storing in a memory of the device a key specific number and a coded key which is calculated by a secret key, the key specific number and a device-specific second predetermined function (col. 3, lines 65-67, col. 4, lines 1-18) and when producing the response reading said specific key number and coded key from the memory, calculating the secret key on the basis of said key-specific number and coded key from the memory using the inverse function of second predetermined function, and utilizing the calculated secret key to produce said response (col. 4, lines 1-15)".

The Examiner asserts that Dolan et al. teaches at col. 3, line 65 to col. 4, line 18 the features (above) not taught by Herve.

Dolan discloses a communication system comprising one or more users and a server. Each user has a security device such as a smart card. The server stores in encoded form the private key for each security device. Each security device stores, or has means for generating, a key encryption key (KEK) unique to the security device. The KEK is used by the server to decrypt the encoded private key of the security device stored in the server. In use, the security device transmits a message to be encrypted by the server and the KEK to the server. The server uses the KEK to decrypt the user's stored encoded private key for encryption of the user's message with the private key.

I. Dolan et al., at col. 3, line 65 to col. 4, line 18, does not teach or suggest storing in a memory of the smart card a key-specific number, and a coded key which has been calculated using the secret key, the key-specific number and a second predetermined function, as asserted

by the Examiner on page 4 of the final Office Action.

Dolan et al. discloses at col. 3, line 65 to col. 4, line 18, two methods for generating a KEK by the security device. In the first method, the KEK is generated by decrypting with a reversible function, an encrypted version of the KEK stored in the security device using a PIN input to security device by the user as key. (col. 3, line 66 to col. 4, line 7). In the second method, the KEK is generated by encrypting with a reversible function a "key" stored in the security device using a random number received from the server as a key.

As described above, Dolan et al. discloses only a single stored number to generate a KEK. Accordingly, Applicant submits that there is no teaching or suggestion in Dolan et al. that both a key specific number and a coded key are stored in the security device, as recited in claims 9, 12 and 14.

Further, there is no teaching or suggestion in Dolan et al. that either the coded KEK or the "key" stored in the security device, are in any way related to the private key of the security device that is stored in the server. Accordingly, Dolan et al. does not teach or suggest storing in a smart card a coded key which has been calculated using the secret key of the security device, as recited in claim 9, 12 and 14.

II. Dolan et al. at col. 3, line 65 to col. 4, line 18 does not teach or suggest calculating with the smart card, the secret key using said key specific number and said coded key by using the inverse function of said second predetermined function, as asserted by the Examiner at page 4 of the final Office Action.

a. Dolan et al. teaches generating a KEK by the security device. The KEK is used in the server to decrypt the encoded private key of the security device which is stored in the server. A KEK is different from the secret key recited in claims 9, 12 and 14. As well understood by those skilled in the art, a secret key is used to encrypt a message while a KEK is used to encrypt the secret key. Accordingly, Dolan et al. does not teach or suggest generating by a smart card, the secret key of the smart card as recited in claims 9, 12 and 14.

b. Dolan et al. teaches generating the KEK by: (1) inputting to the security device a PIN by the user, and using the PIN as a key for decrypting an encrypted version of the KEK stored in the security device (col. 3, line 66 to col. 4, line 7) or (2) inputting to the security

device from the server, a random number and using that random number as a key to encrypt a secret key (not the private key of the security device).

Dolan requires that a PIN or a random number be provided from external to security device to generate a KEK. In contrast to Dolan et al., claims 9, 12 and 14 recite storing in the smart card memory a key specific number and a coded key and calculating the secret key from the stored key specific number and the stored coded key. Accordingly, even if a KEK is asserted to be the same as a secret key (which it is not), there is no teaching or suggestion in Dolan et al. for calculating a secret key from a stored key specific number and a stored coded key as recited in claims 9, 12 and 14.

III. Dolan et al. at col. 3, line 65 to col. 4, line 18 does not teach or suggest utilizing the calculated secret key, the input and the first predetermined function to produce said response with said smart card, as asserted by the Examiner at page 4 of the final Office Action.

Dolan et al. discloses at col. 3, line 65 to col. 4, line 18 outputting from the security device a KEK, based on an input and either a stored coded KEK or a stored "key". Neither the stored KEK or the stored "key" are disclosed as being calculated in the security device. Accordingly, there is no teaching or suggestion in Dolan et al. for producing a response from a smart card utilizing a calculated secret key, as recited in claims 9, 12 and 14.

IV. The incorporation of the features stated by the Examiner as belonging to Dolan et al. into Herve impermissibly changes the principle of operation of Herve (See MPEP 2143.01).

The Examiner asserts at page 4 of the final Office Action that it would have been obvious to one skilled in the art at the time of the invention to incorporate "this feature" of Dolan et al. into Herve.

The Examiner states that the following features of Dolan et al. not found in Herve are to be incorporated into Herve:

a. storing of both a coded secret key and a key specific number in the smart card; and

b. calculating in the smart card the secret key from the stored coded secret key and the key specific number.

Herve stores the secret key and a key specific number (ID) in the smart card. Herve encrypts the secret key for transmission to the authentication terminal with a function

$R = f(S, E \text{ and } In)$, where S is the secret key, E is a random number received from the authentication terminal and In is the ID code.

In order that the combination of Herve and Dolan et al. would meet all the limitations of claims 9, 12 and 14, the combination would at least have to replace the secret key stored in the smart card with a secret key encoded by a function (second predetermined function) other than the function (first predetermined function) used to encode the secret key for transmission to the authentication device. This would in turn, require the addition of an inverse second predetermined function to the smart card.

By incorporating the features of Dolan et al. into Herve, an additional function (decryption of the encrypted secret key) would have to be performed by Herve's smart card. Accordingly, by incorporating the features in Dolan et al. required to meet claims 9, 12 and 14, the Examiner has impermissibly changed the operation of Herve.

Applicant submits that the Examiner has made clear errors in rejecting claims 9, 10, 12 and 14-16 over the combination of Herve and Dolan et al. because Dolan does not teach or suggest the missing features of Herve, that is: (1) storing both a coded secret key and a key specific number in the smart card; (2) calculating a secret key from the coded secret key and a key specific number; and (3) producing a response based on the calculated secret key. Further, even if Dolan et al. taught or suggested the missing features of Herve, the incorporation of these features into Herve would be impermissible because by incorporating these features, the principles by which Herve operates would be impermissibly changed. Accordingly, for all the above reasons, Applicant requests that the rejections to claims 9, 10, 12 and 14-16 be withdrawn and claims 9, 10, 12 and 14-16 be allowed.

Rejection of claims 11 and 13 over Herve, Dolan et al. and WO99/35782 (Kocher)

Claims 11 and 13 depend respectively from allowable claims 10 and 12. Kocher does not make up for the deficiencies of Herve and Dolan et al. Consequently, claims 11 and 13 are allowable at least by their dependency. Accordingly, Applicant requests that the rejection of claims 11 and 13 be withdrawn and claims 11 and 13 be allowed.